



Christina Humphrey Law

February 16, 2023

VIA ECF

Honorable Jacqueline Scott Corley
San Francisco Courthouse, Courtroom E—15th Floor
450 Golden Gate Avenue,
San Francisco, CA 94102

**RE: Denise Droesch, et al. v. Wells Fargo Bank, N.A., Case No. 20-cv-06751-JSC:
Discovery Disputes**

Dear Judge Corley:

Plaintiff hereby submits this joint statement regarding discovery disputes pursuant to the Court's CMC Order dated February 2, 2023. Annexed hereto as Exhibit A is the February 9, 2023 Declaration of Plaintiffs' Expert Ryan Frye, and as Exhibit B is a letter from Defendant to Plaintiffs sent on March 18, 2022. The parties conferred by Zoom on February 8, 2023 in an effort to resolve the dispute and the parties' positions are presented below.

I. Discovery at Issue:

- A) Requests for application data
- B) Production of class data samples

A. Software Time Stamp Preservation and Related Discovery:

Plaintiffs seek production of software log data, including Windows login/logout data¹

Plaintiffs' Position:

Defendant has not adequately investigated the existence of or evidently taken steps to preserve highly relevant software logs, including Windows logs and other logs relevant to establishing Plaintiffs' off-the-clock claims. Plaintiffs have consistently requested software data timestamps such as "[a]ny and all time stamps on software and/or computer systems demonstrating when EMPLOYEES first logged on/off regardless of when clocked into the system." (Plaintiffs' First Set of RFPs, dated January 18, 2021).

During the February 16, 2022 CMC the Court indicated that "**if there is software with time stamp[s] . . . [i]t actually sounds like evidence that both sides would need.**" Doc. No. 109 at 10:20-25 (emphasis added). See *Cadena v. Customer Connexx LLC*, 51 F.4th 831, 840 (9th Cir. 2022) ("booting up their computers at the beginning of their shifts is . . . compensable"). At the March 10th CMC, Defendant indicated that "we are [proceeding] with CIV, Windows, Outlook, Jabber, and Workday." Doc. No. 97 at 43:23-25. The Court limited the scope of the software systems that would be explored in testimony based on its understanding that "[y]ou've got all these other systems and either they're going to show it or not show it. So why don't we deal with all these other ones." *Id.* at 45:3-6.

¹ Plaintiffs also seek (1) amended responses to document requests regarding Defendant's policies for preservation of data, which Defendant has indicated it will provide, and (2) additional 30(b)(6) testimony regarding Defendant's applications and software re: capability to preserve and extent of preservation of data. Per the Court's order, the 30(b)(6) testimony issue will be addressed by the parties in briefing on Defendant's motion for protective order.

Instead of producing all such data, Defendant maintained that “Wells Fargo does not store Windows operating system logs in a database in the ordinary course of business.” Likewise, Defendant maintained that no Outlook or Jabbr usage data is stored. Defendants’ designee on the storage of such data testified that Windows login information is “stored in Windows event logs or other Windows logs” and that such logs are only “kept as long as the Windows operating system allows them to be kept” which is “two days to two weeks.” Below, Defendant suggests it produced “all available reports” for the Plaintiffs. But it elides that most of reports were not available because they were not preserved and, for example, the sum total of all windows login data produced was a couple of days of Ms. Harrison’s logins.

Plaintiffs received expert confirmation that in an enterprise environment with thousands of Windows users, Windows as well as VPN and full disk encryption logging data is not merely stored locally but it is also stored in Domain Controllers and Security and Event Management (“SIEM”) systems which are retained for at least a year for cybersecurity purposes. *See* Declaration of Ryan Frye annexed hereto. Plaintiffs’ expert opined that “Wells Fargo almost certainly retains Windows, VPN, and encryption login/logout data for Class Members and could expeditiously and inexpensively produce such data in this case.” *Id.* ¶ 51. Now, only after Plaintiffs pointed out to Defendant that its own data is stored and retained has Defendant indicated below that it “determined that some data is recorded in association with certain ‘security events’ in a SIEM environment.” But Defendant has to date still not investigated whether it includes the data that Plaintiffs have consistently sought in this case. Moreover, Defendant faults Plaintiff for not requesting VPN or encryption login data when Defendant never revealed that such data exists even though it is clearly responsive to Plaintiffs’ requests.

Ultimately, Plaintiffs seek production of an appropriate sample of relevant data sufficient to establish that Plaintiffs, Opt-ins, and Class Members worked off the clock. In the event that Wells Fargo has not retained relevant and requested data, Plaintiffs intend to file a motion for sanctions up to and including seeking the entry of default judgment pursuant to Rule 37(c)(2)(C). Plaintiffs also intend to seek sanctions based on Wells Fargo’s apparent misrepresentations regarding whether Windows and other data is preserved and can be produced. *See In re Facebook, Inc. Consumer Priv. User Profile Litig.*, 2023 WL 1871107, at *24 (N.D. Cal. Feb. 9, 2023) (sanctioning counsel for refusing to reveal the existence of requested data in an accessible format even if counsel “[p]erhaps . . . were not aware”).

Defendant’s Position:

Plaintiffs’ original discovery requests sought production of “[a]ny and all time stamps on software and/or computer systems demonstrating when EMPLOYEES first logged on/off regardless of when clocked into the system.” Wells Fargo objected to this request as vague, ambiguous, overbroad and burdensome. Plaintiff brought the dispute to the Court, and on March 10, 2022, the Court significantly narrowed the scope and breadth of the request. Wells Fargo produced all available reports for each named Plaintiff from CIV, Windows, Outlook, Jabbr, Softphone/ACES, and Time Tracker/Workday. Wells Fargo then produced eight Rule 30(b)(6) witnesses to testify regarding the type of reports that could be generated from the software applications, as well as the badging system used to enter Defendant’s facilities.

Specifically, Wells Fargo produced a witness on each of the identified software applications to testify (a) how call center employees generally use the software applications, (b) the ways call center employees log into and out of the software applications, (c) whether reports

can be pulled from the software applications, and (d) for how long such reports are available. See March 18, 2022 Letter Re Deposition Topics, attached as Exhibit B.

Plaintiffs now seek additional discovery that goes beyond the scope of their prior requests and the Court's March 10, 2021 ruling. For the first time, Plaintiffs seek data from "Domain Controllers" and "SIEM." After Plaintiffs made these requests in January 2023, Wells Fargo determined that some data is recorded in association with certain "security events" in a SIEM environment. These data are not utilized in the ordinary course of business, and are maintained for cybersecurity functions, such as preventing and investigating potential security breaches, including malware infiltrations. Defendant is investigating whether data indicating when employees logged into or out of CIV, Windows, Outlook, Jabbr, and/or Softphone/ACES can be located and produced from the SIEM. Defendant will continue to meet and confer with Plaintiffs regarding its investigation.²

Plaintiffs, citing to the February 16, 2022 Status Conference transcript, argue that the Court has already found data from the various software applications to be relevant to this case. At the March 10, 2022 Discovery Conference, however, the Court did not make any such finding. Rather, the Court directed Wells Fargo to produce a witness to testify about each software application, so that the parties could obtain evidence regarding *potential* relevance of the data. Plaintiffs do not claim that managers or supervisors reviewed or had access to data showing when employees logged into or out of any software application other than the "Softphone," and therefore data from other programs could not lead to evidence that Defendant was on notice of any possible off-the-clock work. Nor is there any evidence that such data are used with respect to timekeeping practices, or that such data are used in the ordinary course of business. In addition, Plaintiff Harrison testified that she and other phone bankers would perform purely personal tasks after logging into her work computer prior to the start of her shift. Harrison Depo. at 34:6-9, 182:18-183:19, 184:3-16. Thus, the mere fact that an employee has logged into a software program, does not mean she is performing work. An employee could (and indeed many do) log into the Windows operating system and other software applications such as Outlook and Jabbr, and proceed to send personal emails or surf the Internet before taking phone calls from customers.

B. Sample Class Data

Plaintiffs seek documents responsive to Requests for Production Nos. 11 (electronic payroll data that shows hours paid); 17 (timesheet or Time Tracker data); 18 (badge swipe data); 19 (when employees first logged on/off or Windows data); 21 (time sheet (Time Tracker) modification data); 23 (when employees were ready to take calls or Soft phone/Telephony data); 25 (time stamps on software and/or computer systems demonstrating when employees were working). For all the above-referenced data, Plaintiffs have requested that Defendant produce a sample size with a 95% confidence level and with a 5% margin of error.

Plaintiffs' Position³:

Plaintiffs will use the requested samples of class data to establish that Defendant had a

² Plaintiffs mention in this letter and their accompanying expert declaration, "VPN, and encryption login/logout data," but have never made a request for production of such information.

³ Defendant contends that the data requested by Plaintiffs is not requested in any specific RFP. Plaintiffs' requests for data map directly to the corresponding RFP cited in Plaintiffs' statement and represent Plaintiffs' efforts to meet and confer on the scope of those requests.

common policy of not compensating employees for off-the-clock work by, *inter alia*, comparing actual time clocked with badge swipe time and other software time stamp data to the extent such data is preserved (as discussed above) and to establish the quantum of such time. *See, e.g., Owino v. CoreCivic, Inc.*, 36 F.4th 839, 848 (9th Cir. 2022) (“plaintiffs must show “that the whole class suffered damages traceable to the same injurious course of conduct underlying the plaintiffs’ legal theory” by “sufficiently reliable representative or statistical evidence”) (citation omitted).

At the March 10, 2022 CMC, the Court recognized the value of this data, indicating that if “there [are] reports that can be run which would show that she was using the program and at what time. . . . you could compare it to the time records that would show when she was – what time she was being paid for or not.” Doc. 97 at 42:19-22. The Court had previously indicated that production of such data for Plaintiffs is “a good place to start.” Doc. 109 at 12:17-19. The fact that Plaintiff Harrison could not recall when she worked off the clock is irrelevant in light of the fact that actual evidence can establish when she and others were working off the clock.

Defendant puts the cart entirely before the horse. It cites to cases such as *Kazi v. PNC Bank, N.A.*, 2020 WL 607065, at *7 (N.D. Cal. Feb. 7, 2020), where class certification – not discovery – was denied. It argues that Plaintiffs have not provided an expert declaration or model, but Plaintiffs will provide their evidence that the class is in fact certifiable in their class certification motion. *See, e.g., Artis v. Deere & Co.*, 276 F.R.D. 348, 352 (N.D. Cal. 2011) (“the necessary antecedent to the presentation of evidence [that a class action is maintainable] is, in most cases, enough discovery to obtain the material”) (citation omitted).

Defendant’s contention that individual questions will predominate because employees who are logged in and accessing Wells Fargo’s systems are not working is unsupported by the law. Class Members’ workdays began when they booted up their computers to begin working. *See Cadena*, 51 F.4th at 840. Even if that were not the case, the data regarding Class Members’ call readiness and metrics will dispel any anecdotal evidence that Class Members’ logged in for purposes other than performing work. In any event, Defendant misconstrues Plaintiffs’ testimony and declarations. Thompson testified that the metrics impacted her ability to get paid on one of the very pages cited by Defendant. Thompson Depo. 176:17-177:1. And Harrison did not testify that she used Defendant’s computers to regularly conduct personal business nor that she did so after, e.g., accessing customer data, further underscoring the utility of software logs in establishing off-the-clock work. Defendant must produce data that allows Plaintiffs to establish that Class Members routinely were working when they were logged in and not getting paid for that time. *See Tyson Foods, Inc. v. Bouaphakeo*, 577 U.S. 442, 456 (2016) (permitting plaintiff to use “a representative sample to fill an evidentiary gap created by the employer[.]”). The fact that Plaintiffs’ expert could not establish, based on lesser data, when Plaintiffs were working is not a basis for withholding data that can be used to establish when Class Members were working.

Defendant’s burden, inaccessibility, and cost-shifting arguments are impossible to credit because it still does not know whether or where it preserves much of the relevant data and whether there is much burden at all in producing such data from sources it has not yet explored. During the meet and confer process, Plaintiffs’ counsel specifically asked Defendants’ counsel to please provide an explanation of the burden it would endure pulling said data but to date no response has been provided.

Defendant’s Position⁴:

⁴ The RFP numbers and descriptions in Plaintiffs’ position statement do not correspond to any 1117 State Street, Santa Barbara, CA 93101
(805) 618-2924 | (805) 618-2939 (fax) | christina@chumphreylaw.com | www.chumphreylaw.com

While Plaintiffs claim that data from a sample of data for more than 300 employees will “establish that Defendant had a common policy of not compensating employees for off-the-clock work by, *inter alia*, reporting actual time clocked pursuant to the honor system with badge swipe time and other software time stamp data,” they have provided no explanation *how* such data can possibly be used to do so on a class-wide basis given the numerous individualized issues that would need to be resolved for each employee for each day worked. Sample data and the use of “statistics” simply cannot answer these individualized questions, and therefore cannot produce class-wide evidence that Wells Fargo had a uniform policy of permitting off-the-clock work using statistics. *See, e.g., In re: Autozone, Inc.*, 2016 WL 4208200, at *15-16 (N.D. Cal. Aug. 10, 2016) (representational evidence may not establish liability in the absence of a uniform policy affecting all employees and where no common source of evidence exists).

Plaintiffs have presented no expert declaration or model explaining how statistical analyses of the requested sample of data can be used to show that Wells Fargo had a uniform policy permitting off-the-clock work. Plaintiffs themselves testified at deposition that, in general, they accurately recorded their time, and that to the extent they failed to record work time, they did so only occasionally. *See* Thompson Decl. ISO Summary Judgment Opposition ¶ 8; Thompson Depo. at 174:21-176:15, 263:10-24; Harrison Depo. at 53:2-6, 53:13-16, 93:23-94:11. Plaintiff Harrison also testified that she could not identify which days she may have worked off the clock even after being presented with her timekeeping, badge and softphone data. Harrison Depo. At 217:4-8. Even Plaintiffs’ own expert witness at summary judgment disavowed that the data for Plaintiffs that he analyzed could support a claim of actual off-the-clock work. Rather, he could only opine as to “potential” off-the-clock time because he lacked additional information needed to evaluate whether any of that time was actually worked off the clock. *See, e.g.,* ECF No. 129 (Summary Judgment Opposition) at 13–14; *see also* ECF No. 129-4 ¶ 13 & Table 1.

The requested data are also not “reliable in proving . . . the elements of the relevant cause[s] of action” in Plaintiffs’ First Amended Complaint. *Tyson Foods, Inc. v. Bouaphakeo*, 577 U.S. 442, 455 (2016). Other than each employee’s certification of the accuracy of his or her Time Tracker entries, no program or application can conclusively establish whether an employee was performing work at a given time—and no data can establish why an employee recorded the time she did in Time Tracker on any particular day because that determination would require a reconstruction of each day’s work and personal activities. As discussed in section I.A., and as admitted by Plaintiff Harrison, simply because an employee is using her computer and logged into applications, does not mean she is working, as she might be performing purely personal tasks. The data also raise the issue of empirical reliability. Not only does the process of normalizing the time zones of the phone and Time Tracker data that Plaintiffs seek involve separate inquiries into each employee’s location, but because many employees move locations or travel pursuant to Wells Fargo programs, an accurate analysis of this data requires individual assessment of employees’ assignments and physical location on a *daily basis*.

At summary judgment, Plaintiffs could not simply rely on their own data to raise a triable issue of fact regarding the question whether they were working off the clock on any particular

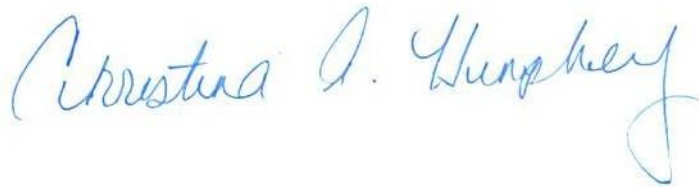
requests served in this case. Based on Plaintiffs’ description and meet and confer communications, Defendant understands Plaintiffs to seek a “sample” of payroll data, Time Tracker data, badge swipe data, Windows login/logout data, Time Tracker adjustment data, Softphone/ACES data, Outlook login/logout data, Jabbr login/logout data, and CIV login/logout data.

day, but instead needed to use emails and declarations to make their case. Plaintiffs therefore will be unable to resolve these individualized issues on a class-wide basis simply by using data from a larger set of employees—such data would only *multiply* the number of individualized issues as to the circumstances of each employee’s conduct on each day worked. This case has been pled as a “class action,” not a “mass action.” In short, Plaintiffs have failed to explain how the requested sample data will either provide “a common source of evidence to determine how much [off-the-clock] time, if any, [employees] engaged in during the proposed class period” or “present a specific model that calculates all class members’ damages.” *Kazi v. PNC Bank, N.A.*, 2020 WL 607065, at *7 (N.D. Cal. Feb. 7, 2020).

In addition to the lack of probative value of the requested data, the burden of collecting and producing the data is substantial. Plaintiffs appear to request a sample of data from multiple sources for more than 300 employees. As Defendant’s 30(b)(6) application witnesses explained, data from Windows, Outlook, and Jabbr is stored locally on employees’ computers and requires an information technology employee to physically retrieve the data from the computer itself. Based on the significant time and disruptive nature associated with completing this process for just one individual, expanding to collect over 300 people would be immensely burdensome.⁵ Given that Plaintiffs have failed to explain how a large sample of data will be used to answer the individualized questions of liability on a class-wide basis, the burden of collecting and producing additional data outweighs any potential use of that information⁶.

Respectfully submitted,

Christina Humphrey Law, PC



Christina A. Humphrey

CC: All Counsel (via ECF)

⁵ To the extent data associated with such applications are available from “SIEM” or “Domain Controllers,” Defendant reserves all rights to make additional objections to Plaintiffs’ requests, including based on the burden to collect and produce such data.

⁶ If the Court were to order Wells Fargo to produce burdensome and costly sampling data, Defendant requests that Plaintiffs bear the cost of that collection and production. *See U.S. ex rel. Carter v. Bridgepoint Educ., Inc.*, 305 F.R.D. 225, 240 (S.D. Cal. 2015) (observing that cost-shifting is appropriate where electronically stored information is inaccessible or the burden or expense of the proposed discovery outweighs the likely benefit).

EXHIBIT A

CHRISTINA HUMPHREY LAW, P.C.

Christina A. Humphrey (SBN 226326)

Robert N. Fisher (SBN 302919)

1117 State Street

Santa Barbara, CA 93101

Telephone: (805) 618-2924

Facsimile: (805) 618-2939

Email: christina@chumphreylaw.com; rob@chumphreylaw.com

QUINTILONE & ASSOCIATES

Richard E. Quintilone, II (SBN 200995)

Jeffrey T. Green (SBN 330065)

22974 El Toro Road, Suite 100

Lake Forest, CA 92630

Telephone: (949) 48-9675

Facsimile: (949) 458-9659

Email: req@quintlawn.com; jtg@quintlawn.com

Attorneys for Plaintiffs Denise Droesch, Shakara Thompson, Kyonna Harrison, and other individuals similarly situated

[Additional Counsel on following page]

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA**

DENISE DROESCH; SHAKARA
THOMPSON; KYONNA HARRISON;
SHANA GOINS; individually, and on behalf
of all others similarly situated,

Plaintiffs,

v.

WELLS FARGO BANK, N.A., and DOES 1
through 100, inclusive

Defendants.

CASE NO. 3:20-cv-06751-JSC

DECLARATION OF RYAN FRYE

GESSNERLAW, PLLC

L. Michelle Gessner (Appearance Pro Hac Vice)

602 East Morehead Street

Charlotte, NC 28202

Telephone: (844) 437-7634

Email: michelle@mgessnerlaw.com

Attorneys for Plaintiffs Denise Droesch, Shakara Thompson, Kyonna Harrison, and other individuals similarly situated

DECLARATION OF RYAN FRYE

Pursuant to 28 U.S.C. § 1746, I, Ryan Frye, hereby declare as follows:

1. I am Senior Vice President of Forensic Services for ModeOne Technologies, Incorporated (“ModeOne”). I am above the age of 18 and am competent to make this declaration. I provide this declaration in connection with a discovery dispute in the above-captioned lawsuit. If asked to do so, I could and would testify consistent with this Declaration at any trial or hearing.

2. I have been retained by litigation counsel for Plaintiffs Denise Droesch, Shakara Thompson, and Kyonna Harrison, in this matter, to provide my expert opinion on Defendant Wells Fargo’s ability to retain and produce data regarding Windows login/logout events and other software login/logout events.

3. ModeOne is being compensated at my standard hourly rate of \$375 per hour for my time spent performing analysis in this matter. The compensation received for this matter is in no way dependent on the outcome of this litigation or on the contents of any particular testimony or opinion that I provide.

4. All of my work on this matter is subject to a confidentiality agreement, which was in place before I was ever provided access to any of the materials referenced herein and I have executed the relevant acknowledgment and agreement to be bound by the Protective Order in this case.

5. Any opinions that I express in this declaration are my opinions as an expert in digital forensics, based on my analysis and review of the evidence described herein. My opinions may be subject to change based on additional evidence or expert opinions that develop in this case, and I reserve the right to amend or supplement my opinions as may be required in response to any future developments.

1 6. Specifically, I have not been able to personally analyze any Wells Fargo device or
2 system. Access to those sources would help me conclusively determine whether Wells Fargo has
3 preserved login/logout event data and the extent to which they could be produced in this case.

4 **1. Background and Qualifications**

5 7. I have an Associate of Applied Science degree in Microcomputer Technology from
6 S.E. College and have obtained the following professional certifications: CCE (Certified Forensic
7 Examiner from the International Society of Forensic Computer Examiners); EnCE (EnCase Certified
8 Examiner); AME (AccessData Mobile Examiner); RCA (Relativity Certified Administrator); and
9 ACE (AccessData Certified Examiner).
10

11 8. I have overseen and/or conducted hundreds of forensic data collection and analysis
12 projects both in the United States and around the world. I am responsible for managing and directing
13 ModeOne's computer forensic lab and for overseeing all of ModeOne's data collection activities,
14 including maintaining chain of custody, secure evidence tracking and storage of client data,
15 reporting and data disposition.
16

17 9. I am a frequent speaker on topics relating to computer forensics and data analysis and
18 am recognized as an expert trainer by AccessData, maker of Forensic Tool Kit, a leading forensic
19 analysis platform widely used by law enforcement and industry professionals.

20 10. I have extensive personal experience creating forensically sound images and
21 conducting forensic analysis on a wide range of digital computing devices including laptops,
22 desktops, servers, cloud infrastructure, tablet computers, mobile phones as well as back-up and
23 storage media.
24

25 11. A current copy of my CV, including a list of all matters in which I have given expert
26 testimony within the previous four years, is attached as Exhibit A to this declaration.

27 **2. Sources of Information**

1 12. I have reviewed Wells Fargo's response to Plaintiffs' Third Requests for Production
2 of Documents, the 30(b)(6) testimony of Wells Fargo designee Brannon Raines, Plaintiffs' meet
3 and confer letter dated January 5, 2023 and Wells Fargo's letter in response dated January 31, 2023,
4 and video of remote login steps.

5 **3. Factual Determinations and Opinions**

6 **A. Background Regarding Security and Logging in Enterprise Environments**

7
8 13. Every time a Windows user logs in or out, the event is recorded locally on the user's
9 computer in a log.

10 14. These local logs may only be retained for a short period of time, which may be as
11 short as two days.

12 15. In an enterprise environment, the login/logout event is not merely a local event on the
13 user's computer.

14 16. Rather, the event is communicated to a server known as a Domain Controller. The
15 Domain Controller exists either in a data center, in the cloud, or both.

16
17 17. Absent use of Domain Controllers, an enterprise would have to manage each
18 computer's login and password individually, which is impossible for an enterprise with thousands
19 of employees.

20 18. The Domain Controller is responsible for the authentication piece of a Windows
21 login, e.g., was the password entered correctly or not? Is the user permitted to log in (yes or no)?
22 These events are recorded across all Domain Controllers. Domain Controllers also record a
23 date/time, username, and IP address as well as other information regarding the login event.

24
25 19. Domain Controllers retain data for specified period of time set by the enterprise.
26
27
28

1 20. When a Windows computer authenticates to a Domain Controller, it follows a
2 specific process to verify the user's credentials and log the login attempt. An example of the process
3 includes:

- 4 a. The user inputs their username and password into the login prompt on their computer.
5 b. The computer sends a request to the domain controller for authentication, including the user's
6 credentials.
7 c. The domain controller validates the credentials against its database of user accounts.
8 d. If the credentials are valid, the domain controller returns a token to the computer, indicating
9 that the user has been authenticated.
10 e. The computer caches the token for future use and grants the user access to the network
11 resources.
12 f. The Domain Controller confirms that the login credentials are valid.

13 21. In order to maintain proper records for cybersecurity purposes, identify security
14 incidents, and assist in compliance reporting, the Domain Controller transfers login/logout data to a
15 Security Information and Event Management ("SIEM") system where the data is maintained in
16 aggregated logs.

17 22. An SIEM aggregates and correlates log data from various sources such as firewalls,
18 intrusion detection systems, and endpoints (including physical machines such as desktops), to
19 identify security incidents and help in compliance reporting.

20 23. The SIEM will maintain Windows login data such as username, date and time, the IP
21 address of the computer logging in, the computer serial number or other ID, and whether the login
22 attempt was successful.

23 24. In addition to maintaining aggregate logs of Windows events, the SIEM will keep
24 other security data, such as Virtual Private Network ("VPN") login data.

25 25. VPN's are used by remote workers to ensure all network activity is contained within
26 a company's internal network.
27
28

1 26. SIEM's also retain other data such as disk encryption software logins that are used in
2 enterprises such as financial institutions to secure data on individual devices.

3 27. Retaining user authentication events in a SIEM (Security Information and Event
4 Management) system is critical for adequate intrusion analysis and breach response.

5 28. Having access to a comprehensive and historical view of user authentication events
6 enables security experts to identify patterns and anomalies that may indicate a security breach.

7 29. This information is particularly important in identifying the scope of a breach and
8 determining the source of the attack, as well as understanding the timeline of the intrusion.

9 30. Retaining user authentication events for over a year is now standard practice in the
10 security industry and can be easily achieved through commercially available applications. This
11 wealth of data provides a solid foundation for thorough and accurate security analysis, enabling
12 organizations to respond quickly and effectively to potential security incidents.

13 31. In this regard, most data breaches are not discovered for, on average, 212 days.
14 Accordingly, SIEM data must be maintained for lengthy periods to ensure that data breaches can be
15 appropriately investigated.

16 32. SIEM data can easily be filtered, manipulated, and produced in litigation.

17 33. In fact, the National Institute of Standards and Technology ("NIST") cybersecurity
18 framework specifies that "[l]ogs often need to be preserved to meet legal or regulatory
19 requirements."¹

20 34. Even if specific logs are not being recorded or retained prior to the litigation, an
21 enterprise can easily modify its Domain Controller, Endpoint Detection and Response ("EDR"), and
22 SIEM settings to capture and retain relevant data.

23
24
25
26
27
28

¹ <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf> at 3-3

35. For example, one commonly used Endpoint Detection and Response solution is called Carbon Black Cloud Endpoint Standard (“Carbon Black”).

36. Carbon Black provides online instructions for exporting audit logs including log in attempts.²

g. Wells Fargo Almost Certainly Retains Aggregated Log Data in a SIEM

37. Wells Fargo’s counsel has indicated that Wells Fargo “does not store Windows operating system logs in a database in the ordinary course of business.”

38. Wells Fargo’s 30(b)(6) deponent on the subject testified that Windows login data is maintained on individual computers and is typically retained for “two days to two weeks.”

39. In my opinion, it is extremely likely that Wells Fargo does retain security event data including Windows, VPN, and encryption login/logout data in a SIEM.

40. In the first instance, Wells Fargo, as a large financial institution, must monitor its systems for data breaches and, as discussed above, it is standard industry practice to use a SIEM for this purpose.

41. Moreover, it would be completely impractical for Wells Fargo to manage any portion of its operation with thousands of employees such as the class members in this case with individual logins set on a computer-by-computer basis.

42. Further, there is significant evidence that Wells Fargo uses Domain Controllers and SIEMs.

43. Wells Fargo job listings for IT positions specify that applicants should have “[e]xperience with enterprise security technologies such as SIEM,”³ and “[h]ands-on experience with information security tools such as an enterprise SIEM solution.”⁴

² <https://developer.carbonblack.com/reference/carbon-black-cloud/cb-defense/latest/rest-api/>

³ <https://www.wellsfargojobs.com/en/jobs/r-214548/senior-information-security-engineer-cyber-threat-intelligence/>

⁴ https://ninjajobs.org/job/696e027fa3045ae4357f?utm_source=reddit&utm_medium=social&utm_campaign=auto_post

44. Indeed, Wells Fargo employees have spoken openly about the company's use of SIEM software. As early as 2008, Denis Hein, a senior information security engineer for Wells Fargo was quoted regarding best practices for SIEM implementation.⁵

45. In 2021, Gary Howell, a Cyber Security Expert at Wells Fargo, spoke as a panelist on the subject of "The Importance of SIEM and Cyber Resiliency."⁶

46. Also in 2021, VMware, Inc., the maker of Carbon Black, spoke at Wells Fargo's annual TMT Summit about Carbon Black and other products.⁷

47. Moreover, based on Plaintiff Kyonna Harrison's experience, Wells Fargo uses PulseSecure VPN for Class Members who log in remotely.

48. PulseSecure VPN promotes "easy integration" with SIEM software.⁸

49. Likewise, Wells Fargo uses a SecureDoc disk encryption solution which requires a user to log in each time they boot up their computer before Windows can be loaded.

50. SecureDoc's enterprise solution integrates with Active Directory allowing login data to be captured and aggregated.⁹

51. Accordingly, in my opinion, Wells Fargo almost certainly retains Windows, VPN, and encryption login/logout data for Class Members and could expeditiously and inexpensively produce such data in this case.

I declare the foregoing to be true under penalty of perjury of the laws of the State of California and the United States of America. Executed this 9th day of February 2023.

Ryan Frye

Ryan Frye, Declarant

⁵ <https://www.networkworld.com/article/2276855/four-tips-for-siem-success.html>

⁶ <https://tec-refresh.com/events/the-importance-of-siem-and-cyber-resiliency/>

⁷ <https://seekingalpha.com/article/4472900-vmware-inc-vmw-presents-annual-virtual-wells-fargo-tmt-summit-transcript>

⁸ https://docs.pulsesecure.net/WebHelp/PCS/8.3R1/Content/PCS/PCS_AdminGuide_8.3/Logging_Overview.htm

⁹ <https://winmagic.com/en/products/full-disk-encryption-for-windows/>

EXHIBIT B

MUNGER, TOLLES & OLSON LLP

RONALD L. OLSON
ROBERT E. DENHAM
JEFFREY I. WEINBERGER
CARY B. LERMAN
GREGORY P. STONE
BRAD D. BRIAN
BRADLEY S. PHILLIPS
GEORGE M. GARVEY
WILLIAM D. TEMKO
JOHN W. SPIEGEL
DONALD B. VERRILLI, JR. P.C.*
TERRY E. SANCHEZ
STEVEN M. PERRY
MARK B. HELM
JOSEPH D. LEE
MICHAEL R. DOYEN
MICHAEL E. SOLOFF
KATHLEEN M. McDOWELL
GLENN D. POMERANTZ
THOMAS B. WALPER
HENRY WEISSMANN
KEVIN S. ALLRED
JEFFREY A. HEINTZ
JUDITH T. KITANO
JEROME C. ROTH
GARTH T. VINCENT
TED DANE
STUART N. SENATOR
MARTIN D. BERN
ROBERT L. DELL ANGELO
JONATHAN E. ALTMAN
KELLY M. KLAUS
DAVID B. GOLDMAN
DAVID H. FRY
LISA J. DEMSKY
MALCOLM A. HEINICKE
JAMES C. RUTTEN
RICHARD ST. JOHN
ROHIT K. SINGLA
CAROLYN HOECKER LUEDTKE
C. DAVID LEE
ERETT J. RODDA P.C.*
KATHERINE M. FORSTER
BLANCA FROMM YOUNG
SETH GOLDMAN
GRANT A. DAVIS-DENNY
JONATHAN H. BLAVIN
DANIEL B. LEVIN
MIRIAM KIM
MISTY M. SANFORD
HAILYN J. CHEN
BETHANY W. KRISTOVICH

JACOB S. KREIKAMP
JEFFREY Y. WU
LAURA D. SMOLOWE
ANJAN CHOUDHURY
KYLE W. MACH
HEATHER E. TAKAHASHI
ERIN J. COX
BENJAMIN J. HORWICH
E. MARTIN ESTRADA
BRYAN H. HECKENLIVELY
ELAINE J. GOLDENBERG P.C.*
GINGER D. ANDERS P.C.*
MARGARET S. MARASCHINO
JOHN M. GILDERSLEEVE
ADAM B. WEISS
KELLY L. C. KRIEBS
JEREMY A. LAWRENCE
LAURA K. LIN
ACHYUT J. PHADKE
ZACHARY M. BRIERS
JENNIFER M. BRODER
KURUVILLA J. OLASA
JUSTIN P. RAPHAEL
ROSE LEDA EHLE
JOHN W. BERRY
ROBYN K. BACON
JORDAN D. SEGALL
JONATHAN KRAVIS*
KAREN A. LORANG
JOHN L. SCHWAB
EMILY C. CURRAN-HUBERTY
MATTHEW S. SCHONHOLZ
AIMEE M. CONTRERAS-CAMUA
L. ASHLEY AULL
WESLEY T.L. BURRELL
CRAIG JENNINGS LAVOIE
JENNIFER L. BRYANT
NICHOLAS D. FRAM
TYLER HILTON
VINCENT LING
JESSICA REICH BARIL
JULIANA M. YEE
JEREMY K. BEECHER
MATTHEW K. DONOHUE
JOHN B. MAJOR
LAUREN C. BARNETT
NICK R. SIDNEY
C. HUNTER HAYES
SKYLAR B. GROVE
SARAH S. LEE
LAURA M. LOPEZ

350 SOUTH GRAND AVENUE
FIFTIETH FLOOR
LOS ANGELES, CALIFORNIA 90071-3426
TELEPHONE (213) 683-9100
FACSIMILE (213) 687-3702

560 MISSION STREET
TWENTY-SEVENTH FLOOR
SAN FRANCISCO, CALIFORNIA 94105-3089
TELEPHONE (415) 512-4000
FACSIMILE (415) 512-4077

601 MASSACHUSETTS AVENUE NW
SUITE 500E
WASHINGTON, D.C. 20001-5369
TELEPHONE (202) 220-1100
FACSIMILE (202) 220-2300

March 18, 2022

COLIN A. DEVINE
DANE P. SHIKMAH
LEXI PEACOCK
MAGGIE THOMPSON
SAMUEL H. ALLEN
ALLISON M. DAY
GIOVANNI S. SAARMAN GONZALEZ
STEPHANIE G. HERRERA
TERESA REED DIPPO
DANIEL BENYAMIN
SARA A. MCDERMOTT
J. MAX ROSEN
RACHEL G. MILLER-ZIEGLER*
ANNE K. CONLEY
DAVID W. MORESHEAD
ANDREW W. BREWSTER III
ROWLEY J. RICE
DAHLIA MIGNOUNA*
BRANDON R. TEACHOUT
USHA CHILUKURI VANCE
ALEXANDER S. GORIN
ZARA BARI
BRENDAN B. GANTS*
MARI T. SAIGAL
LAUREN E. ROSS*
BENJAMIN G. BAROKH
ABE DYK
MICHELE C. NIELSEN
APRIL YOUNG-ROLL
COBUS VAN DER VEEN*
MEGAN MCCREADIE
STEPHEN HYLAS
ARIEL TESHUVA
SHANNON GALVIN AMINIRAD
LLOYD MARSHALL
XIAONAN APRIL HU*
NATALIE KARL
BRANDON MARTINEZ
ERINMA E. KALLU
ANDREW LEWIS
CARRIE C. LITTEN
RUBY J. GARRETT*
JAMES R. SALZMANN
ELIZABETH DOUGLAS
SAMIR HALAWI
ROBIN S. GRAY
MICA L. MOORE
JOSEPH MOSES
MICHAEL I. SELVIN
ALICE X. WANG
HUNTER V. ARMOUR

NATHANIEL F. SUSSMAN
PAUL E. MARTIN
REBECCA L. SCIARINO
CORY M. BATZA
BRIAN R. BOESSENECKER
AVI REJWAN OVED
ROBERT E. BOWEN
RICHARD T. JOHNSON
GRACE DAVIS FISHER
CALEB W. PEIFFER
ANDRÉS CANTERO, JR.
JAMIE B. LUGURI
STEVEN B. R. LEVICK
SARA H. WORTH
NATALIE G. MOYCE
WILLIAM M. ORR
GABRIEL M. BRONSHTEYN
ALEX C. WERNER
ROSIO FLORES
JESSICA O. LAIRD
ERICA C. TOOCH
EVAN MANN
ANDREW T. NGUYEN
RACHEL M. SCHIFF
MIRANDA E. REHAUT

OF COUNSEL

ROBERT K. JOHNSON
PATRICK J. CAFFERTY, JR.
PETER A. DETRE
BRAD SCHNEIDER
PETER E. GRATZINGER
JENNY H. HONG
KIMBERLY A. CHI
ADAM R. LAWTON
MICHAEL E. GREANEY
SARAH J. COLE

E. LEROY TOLLES
(1922-2008)

*ADMITTED IN DC.
ALL OTHERS ADMITTED IN CA

Writer's Direct Contact
(213) 683-9220
(213) 683-9220 FAX
martin.bern@mto.com

VIA ELECTRONIC MAIL ONLY

Richard E. Quintilone
Quintilone & Associates
req@quintlaw.com

Re: 30(b)(6) Deposition Topics as Narrowed in Meet & Confer and by the Court

Dear Counsel:

In order to document the deposition topics that will be at issue in the upcoming Rule 30(b)(6) deposition of Wells Fargo Bank, N.A., we are providing you with an updated tracking chart that shows the original topic, the agreement of counsel to change or narrow such topics during the meet and confer between Ms. Humphrey and Mr. Bern, and additional limitations placed on certain topics by the Court at the informal discovery hearing.

For the topics on which Wells Fargo's witness will testify on March 24, 2022, the deponent will be prepared to address all business lines at Wells Fargo. These topics are highlighted in green. For those topics highlighted in yellow, the witness will only be testifying as to the Consumer and Small Business Banking line of business. As we have stated previously, if you want to take additional depositions for other lines of business on these topics, please inform us as soon as possible.

MUNGER, TOLLES & OLSON LLP

Richard E. Quintilone
 March 18, 2022
 Page 2

In addition, we request that Plaintiffs serve a formal Notice of Deposition for March 24, 2022, as we have only received a draft notice from you previously. We request that the notice take into account the information from the meet and confer and the Court's direction at the discovery conference, as reflected in the attached chart.

Topic	Original Topic in Draft Notice	Agreed Amended Topics from Meet & Confer	Topics as Limited by Court
1	The person or persons most qualified to testify regarding the organizational structure of all Wells Fargo Call Centers (in relation to Wells Fargo Bank, N.A. and how it fits into the overall structure), including the reporting and decision-making structure, membership and hierarchy, as well as the identity, duties, and positions held by corporate employees with direct or indirect authority over EMPLOYEES, including but not limited to: (Plaintiffs are willing to accept a declaration with a chart for certain sub-categories for efficiency purposes).	List of call center locations, the line of business under which each call center operates, the number of phone bankers at each call center, and in which call centers team members who opted into the FLSA collective worked during the relevant time period.	Plaintiffs will serve an interrogatory (26:10)

MUNGER, TOLLES & OLSON LLP

Richard E. Quintilone
March 18, 2022
Page 3

1A	The names, jobs positions, and dates of employment of employees with direct and indirect authority over EMPLOYEES during the RELEVANT TIME PERIOD at each of the Call Centers within the FLSA COLLECTIVE, ARIZONA, CALIFORNIA, AND NORTH CAROLINA CLASSES;	Plaintiffs will serve an interrogatory on topics 1, 1C, 1E, 1F, 1G, and we will revisit 1A, 1B, and 1D after a response is provided.	
----	--	--	--

MUNGER, TOLLES & OLSON LLP

Richard E. Quintilone

March 18, 2022

Page 4

Topic 1B	The types of services rendered by EMPLOYEES in the call centers, the number of departments, management structure/hierarchy, number of employees and types of employees at each location, software used at each location by EMPLOYEES, hours of operation at each location; desk equipment set up; and badging practices at each location (basically how do you get in and out of building);	Plaintiffs will serve an interrogatory on topics 1, 1C, 1E, 1F, 1G, and we will revisit 1A, 1B, and 1D after a response is provided.	
Topic 1C	How the locations are staffed of EMPLOYEES and if any staffing software is used to staff the locations and how that staffing software works	How the shift scheduling of call center employees is performed and any procedures in place to ensure such scheduling occurs in compliance with applicable state/federal law.	
Topic 1D	Whether each location has a budget and what categories comprise the budget for each call center (broad categories);	Plaintiffs will serve an interrogatory on topics 1, 1C, 1E, 1F, 1G, and the parties will revisit 1A, 1B, and 1D after a response is provided.	

MUNGER, TOLLES & OLSON LLP

Richard E. Quintilone
 March 18, 2022
 Page 5

Topic 1E	The entity or department that maintains and/or processes payroll and time data for PLAINTIFFS and EMPLOYEES;	Plaintiffs will serve an interrogatory requesting the title of the department that maintains and processes payroll information and whether that maintenance and processing is done in-house.	
Topic 1F	A list of all locations nationwide where call centers are located during the RELEVANT TIME PERIOD	List of call center locations during the relevant time period applicable to each area of the country in which such call centers are located.	Plaintiffs will serve an interrogatory (26:10)
Topic 1G	The estimated number of EMPLOYEES in the ARIZONA CLASS, CALIFORNIA CLASS, AND NORTH CAROLINA CLASS.	An estimated number of putative class members in each of the three putative state law classes during the relevant time period for each.	Plaintiffs will serve an interrogatory (26:10)
Topic No. 2	The person or persons most qualified to testify as to EMPLOYEES job duties and responsibilities during the RELEVANT TIME PERIOD, including but not limited to	The different types of job duties performed by front-line call center employees in California, Arizona, North Carolina and states where employees who opted into the FLSA collective worked.	
Topic 2A	The tasks EMPLOYEES were expected to perform and how;	The different types of job duties generally performed by front-line call center employees in states where employees	

MUNGER, TOLLES & OLSON LLP

Richard E. Quintilone

March 18, 2022

Page 6

		who opted into the FLSA collective worked.	
Topic 2B	A description of any and all job descriptions applicable to EMPLOYEES during the RELEVANT TIME PERIOD.	A witness to authenticate generally the job descriptions that correspond to jobs held by the call center employees in Topic 2, if served an interrogatory requesting the production of those descriptions.	
Topic 2C	A list and description of all software systems that EMPLOYEES use to complete their job duties and responsibilities including but not limited to Teamworks, BCS, CIV, SOTA, Softphone, Hogan, VL, DAT, Skype, Visa, IES, Aspect System, PSVI, and Timetracker (as well as any not listed here).	How call center employees generally use Softphone/ACES, Timetracker/Workday, CIV, Windows, Outlook, and Jabbr to complete their job duties and responsibilities.	Limited by the Court to the badging system, Softphone/ACES, Timetracker/Workday, CIV, Windows, Outlook, and Jabbr. (42:14-25, 43:1, 45:1-2)
Topic 2D	All steps the EMPLOYEES take to log on and out of any software systems discussed in c above;	The different ways that call center employees could log into and log out of Softphone/ACES, Timetracker/Workday, CIV, Windows, Outlook, and Jabbr while working in a call center.	

MUNGER, TOLLES & OLSON LLP

Richard E. Quintilone

March 18, 2022

Page 7

Topic 2E	All training that EMPLOYEES undergo for job duties and responsibilities and for software systems discussed in c above (the operational manuals for c was requested in Plaintiff's RPD 6 and 7, please make sure those are produced well in advance of this deposition).	The training the named Plaintiffs underwent to log into and log out of Softphone/ACES, Timetracker/Workday, CIV, Windows, Outlook, and Jabbr while working in a call center.	
Topic No. 3	The person or persons most qualified to testify as to DEFENDANTS policies and practices regarding meal and rest breaks in California during the RELEVANT TIME PERIOD, including but not limited to the following:	No changes	
Topic 3A	The substance of the policies, and any changes made to said policies and how the policies are communicated to the CALIFORNIA CLASS;	Defendant's meal and rest period policies during the relevant time period, and how those policies were communicated to employees.	
Topic 3B	Timekeeping and recording of meal breaks;	No changes	
Topic 3C	Location of timeclocks within the facilities;	No changes	
Topic 3D	Accessibility and location of rest areas including restrooms, break rooms, outdoor facilities; and if security clearances were needed before entering in and out of work stations;	The general layout of call center facilities and security practices for entering and exiting the buildings at Defendant's call center locations.	
Topic 3E	Any meal period waivers in effect;	Any meal period waivers in effect involving call center employees.	

MUNGER, TOLLES & OLSON LLP

Richard E. Quintilone
 March 18, 2022
 Page 8

Topic 3F	Defendant's meal and rest period premium payment policy, if any, and how premium payments are reported and processed;	No changes	
Topic 3G	Any and all databases recording meal and rest breaks taken and/or waived;	The manner in which call center employees report whether they took compliant meal and rest periods, and how such reporting information is stored and maintained.	
Topic 3H	The substance of said databases (field definitions and what they mean);	No changes	
Topic 3I	Defendant's enforcement of policies for meal and rest breaks;	No changes	
Topic 3J	Any applicable exemptions that apply to CALIFORNIA CLASS for meal breaks during the RELEVANT TIME PERIOD;	Whether Defendant has received any meal break exemptions for its California call center employees from the California Department of Industrial Relations.	.
Topic 3K	Whether or not DEFENDANT'S have conducted an investigation, audit, or the like regarding meal and rest breaks as to the CALIFORNIA CLASS or management of CALIFORNIA CLASS and what was done;	No changes	
Topic 3L	Whether or not DEFENDANT'S have litigated its meals and rests break policies as they pertain to other EMPLOYEES in California, whether in an administrative or court	Whether it can readily be determined if Defendant's meal and rest break policies specific to California call center employees	

MUNGER, TOLLES & OLSON LLP

Richard E. Quintilone

March 18, 2022

Page 9

	proceedings, the names and outcome of any proceedings	have been previously litigated and, if so, any publicly available judicial decisions that addressed compliance of such policies with federal or state law.	
Topic 3M	A description of any internal communications regarding compliance of DEFENDANT'S meal and rest breaks policies/practices with California law;	A description of any internal and non-privileged, high-level communications regarding changes made to Defendant's meal and rest break policies for purposes of compliance with California law.	
Topic 3N	Any and all complaints made to Human Resources and/or any similar department or 800 number made by other EMPLOYEES regarding meal and rest breaks;	Whether complaints are coded for alleged meal and rest break policy violations and, if they are, the general content of complaints coded in that manner.	Defendant is still investigating whether it is possible to search and the parties can further meet & confer on this topic once that investigation concludes. (28:10-12)
Topic 3O	The names of all EMPLOYEES (including supervisors/managers) terminated for violating meal and/or rest period policies of DEFENDANT.	Whether termination records are coded for meal and rest break policy violations and, if they are, what call center employee terminations were coded for meal and rest break and timekeeping policy violations generally.	

MUNGER, TOLLES & OLSON LLP

Richard E. Quintilone
 March 18, 2022
 Page 10

Topic No. 4	The person or persons most qualified to testify as to DEFENDANT'S policies, practices, and procedures for tracking the time spent by EMPLOYEES and EMPLOYEES performing tasks during the RELEVANT TIME PERIOD, including but not limited to the following:	The person or persons most qualified to testify as to Defendant's policies for tracking the time worked by call center employees.	
Topic 4A	The identification, management, maintenance, storage, development, and operation of DEFENDANT'S software/database/electronically-stored information that contain time records for the RELEVANT TIME PERIOD for EMPLOYEES including but not limited to any applications used by employees to track time and other applications that may contain time stamps for employees including but not limited to badging access in and out of DEFENDANT'S worksites, login data if EMPLOYEES dial in remotely, Teamworks, BCS, CIV, SOTA, Softphone, Hogan, VL, DAT, Skype, Visa, IES, Aspect System, PSVI, and Timetracker;		Limited by the Court to the process by which data is collected in and whether reports can be pulled from the badging system, Softphone/ACES, Timetracker/Workday, CIV, Windows, Outlook, and Jabbr. (42:14-25, 43:1, 45:1-2)
Topic 4B	DEFENDANT'S efforts to track, calculate, and/or document hours of work performed by EMPLOYEES during the RELEVANT TIME PERIOD;	Any software application(s) used to document for the purpose of payroll calculations the hours worked by call center employees during the relevant time period.	

MUNGER, TOLLES & OLSON LLP

Richard E. Quintilone

March 18, 2022

Page 11

Topic 4C	DEFENDANT'S policies, procedures, and practices regarding timekeeping, recording of time, and/or submission of time and/or off-the-clock time of all EMPLOYEES during the RELEVANT TIME PERIOD including the communication of those policies to EMPLOYEES;	No changes	
Topic 4D	DEFENDANT'S policies, procedures, and practices regarding clocking in and out at the locations worked by EMPLOYEES including the location of time clocks in relation to workstations and any pre- and post-shift activities;	No changes	
Topic 4E	Any investigations performed or reports created regarding DEFENDANT'S timekeeping and/or compensation policies and practices pertaining to EMPLOYEES in the last seven (7) years;	WITHDRAWN	
Topic 4F	DEFENDANT'S policies, procedures, and practices pertaining to time worked by EMPLOYEES during the RELEVANT TIME PERIOD outside of the time reflected on work schedules, including, but not limited to, before the beginning of their paid shifts, before clocking in or otherwise logging on to any timekeeping system, while traveling between DEFENDANT'S designated work stations, after clocking out or otherwise logging out of any timekeeping system, during meal and rest breaks.	Defendant's timekeeping policies generally.	

MUNGER, TOLLES & OLSON LLP

Richard E. Quintilone
 March 18, 2022
 Page 12

Topic 4G	The substance of all databases tracking time of EMPLOYEES including the definitions of all fields and overall meaning of numbers contained within said databases (including the attached as Exhibits, Plaintiffs are expecting data dictionaries be produced well in advance of the deposition, the witness should be able to testify as to what fields are not included on the exhibits and how the data was exported);	The recordation and storage of data regarding time entered into software programs as time worked by call center employees.	
Topic 4H	DEFENDANT'S recordkeeping retention policies regarding all of the above;	Defendant's retention policies for data reflecting time worked by its call center employees as reported by them through the use of software programs.	
Topic 4I	Whether DEFENDANT has received complaints, internal or external, regarding its timekeeping policies or off-the clock work from call center employees during the RELEVANT TIME PERIOD, how such complaints are recorded by DEFENDANT and what, if any follow up or resolutions have resulted;	Whether complaints are coded for alleged meal and rest break or timekeeping policy violations and, if they are, the general content of complaints coded in that manner.	Defendant is still investigating whether it is possible to search and the parties can further meet & confer on this topic once that investigation concludes. (28:10-12)
Topic 4J	Whether DEFENDANT sought legal counsel in the creation of and/or changes made to its timekeeping systems at any point in the last seven (7) years;		Objection sustained by Court (5:1-5)
Topic 4K	Whether any Department of Labor, Court, administrator, and/or arbitrator has determined that DEFENDANT'S timekeeping systems do not	No changes	

MUNGER, TOLLES & OLSON LLP

Richard E. Quintilone
 March 18, 2022
 Page 13

	comply with Arizona, California, North Carolina, or federal law;		
Topic 4L	Whether any Department of Labor, Court, administrator, and/or arbitrator has determined that a call center employee worked off the clock (or in turn did not work off the clock) under Arizona, California, North Carolina, or federal law;	Whether any records regarding administrative, arbitral or judicial decisions are coded for off-the-clock claims and, if so, whether those records show generally that a call center employee was determined to have worked off the clock by a Court, the Department of Labor, or an arbitrator.	
Topic 4M	A description of any internal communications regarding compliance of DEFENDANT'S timekeeping systems with Arizona, California, North Carolina, or federal law and/or changes made to timekeeping system at any point in the last seven (7) years.	Any non-privileged, high-level communications of Defendant's regarding compliance of or changes made to Defendant's timekeeping systems during the relevant time period.	
Topic 4N	A description of any internal communications regarding off the clock work performed by EMPLOYEES or policies pertaining thereto;	Defendant's policies prohibiting off-the-clock work.	
Topic 4O	Whether any EMPLOYEES or managers of EMPLOYEES have been terminated for working off the clock or encouraging work off the clock or changing the time recorded of EMPLOYEES;	Defendant's policies prohibiting off-the-clock work.	

MUNGER, TOLLES & OLSON LLP

Richard E. Quintilone
 March 18, 2022
 Page 14

Topic No. 5	The person or persons most qualified to testify regarding DEFENDANT'S policies, practices, and procedures regarding its payroll calculations and payroll database for EMPLOYEES, including but not limited to the following:	No changes	
Topic 5A	Calculation of meal and rest period premiums in California;	Whether meal and rest period premiums are paid as required by California law and at what rate.	
Topic 5B	Whether any meal or rest periods have been paid in California and if so, how much during the RELEVANT TIME PERIOD;	Whether meal and/or rest period premiums have been paid to the named plaintiff in California during the relevant time period.	
Topic 5C	Calculation of pay upon involuntary or involuntary termination in California;		Struck by Court (7:2-12)
Topic 5D	The identification, management, maintenance, storage, development and operation of DEFENDANT'S software/database/electronically-stored information that contains payroll data for the RELEVANT TIME PERIOD for EMPLOYEES;	The general process by which payroll data is stored and maintained for call center employees during the relevant time period .	
Topic 5E	DEFENDANT'S recordkeeping retention policies regarding all of the above.	Defendant's data retention policies for payroll data of call center employees maintained during the relevant time period.	

MUNGER, TOLLES & OLSON LLP

Richard E. Quintilone

March 18, 2022

Page 15

Topic No. 6	The person or persons most qualified to testify as to any and all wage statements distributed to PLAINTIFF and/or CALIFORNIA CLASS during the RELEVANT TIME PERIOD, including but not limited to the following:		Struck by Court (15:4-10)
Topic 6A	A description of any and all versions of the wage statements during the RELEVANT TIME PERIOD and any changes made thereto;		Struck by Court (15:4-10)
Topic 6B	The definitions of the items on the wage statements including employer name;	The information contained in the wage statements provided to the named class representatives in California and Arizona for the relevant time period generally.	
Topic 6C	The policies and procedures implemented for issuing final wages statements and pay;		Struck by Court (20:4-6)
Topic 6D	The timing of issuance of wages and pay statements;		Limited by the Court to whether wages are issued bi-weekly. (20:4-6)
Topic 6E	Identification and description of the electronic data source from which the information on the wage statement is based and how it is translated into a wage statement;		Limited by the Court to the identification and description of the database from which timekeeping information is pulled to populate wage statements and how any time

MUNGER, TOLLES & OLSON LLP

Richard E. Quintilone
 March 18, 2022
 Page 16

			adjustments are reflected in that database. (24:3-7)
Topic 6F	Whether DEFENDANTS have received complaints regarding its wage statements from other EMPLOYEES during the RELEVANT TIME PERIOD;		Struck by Court (17:7-13)
Topic 6G	Whether DEFENDANTS sought legal counsel in the creation of and/or changes made to its wage statement;		Struck by Court (17:3-13)
Topic 6H	Whether any Department of Labor, Court, administrator, or arbitrator has determined that DEFENDANT'S wage statement does not comply with California law;		Struck by Court (17:11-13; 20:4-6)
Topic 6I	A description of any internal communications regarding compliance of DEFENDANT'S wage statement with California law.		Struck by Court (18:6-25)
Topic No. 7	The person or persons most qualified to testify as to managers' job duties and responsibilities as it pertains to PLAINTIFFS and/or EMPLOYEES during the RELEVANT TIME PERIOD, including but not limited to the following:	The general duties and responsibilities of supervisors of the named plaintiffs with regard to timekeeping, including the taking and recording of meal and rest periods taken or missed.	

MUNGER, TOLLES & OLSON LLP

Richard E. Quintilone
 March 18, 2022
 Page 17

Topic 7A	The managers' role in supervising EMPLOYEES as it pertains to time tracking and enforcing policies as to meal and rest breaks and wage statements and payment upon termination in California, and off the clock policies in nationwide.	The general duties and responsibilities of supervisors of the named plaintiffs with regard to timekeeping, including the taking and recording of meal and rest periods taken or missed.	
Topic 7B	Any training managers' received on those policies;	The general training of supervisors of the named plaintiffs regarding timekeeping, including the taking and recording of meal and rest periods taken or missed.	
Topic 7C	The policies regarding work of overtime at the Call Centers, including enforcement of policies and budgets (if any) as they pertain to overtime hours;	Defendant's policies regarding overtime work for its call center employees during the relevant time period.	
Topic 7D	Any and all bonuses or incentives received managers and what activities they are tied to (e.g., meeting budgets, etc.);	Any bonuses or incentives paid to supervisors or managers of the named plaintiffs that are tied to meeting labor budgets.	
Topic 7E	The policies and procedures for changing time of an EMPLOYEE and where that is reflected in the software systems.	As it relates to the supervisors of the named plaintiffs, whether a supervisor can change the time entered by a call center employee once it has been certified as true and accurate, and then submitted by the employee for approval and payment.	

MUNGER, TOLLES & OLSON LLP

Richard E. Quintilone
 March 18, 2022
 Page 18

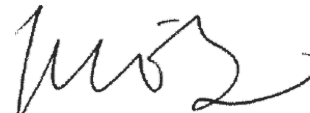
Topic 7F	Whether any managers of EMPLOYEES have been terminated for violating any DEFENDANT'S policies for meal and rest breaks, wage statements, payment upon termination, off the clock, or changing an employee's time during the RELEVANT TIME PERIOD.	Whether termination records are coded for meal and rest break policy violations and, if they are, what call center employee terminations were coded for meal and rest break and timekeeping policy violations generally.	
Topic No. 8	The person or persons most qualified to testify as to EMPLOYEES job duties and responsibilities, work stations, and expenses while working from home during the RELEVANT TIME PERIOD, including but not limited to:	The general job duties and responsibilities of, and the equipment generally provided to, call center employees while working from home during the relevant time period as a result of the pandemic.	Limited further by Court to exclude any topics relating to expense reimbursement. (26:7-8)
Topic 8A	The Process by which EMPLOYEES working from home log into the various software systems and what time stamps are recorded and how employees are monitored;	The general login process for call center employees working from home during the relevant time period as a result of the pandemic.	
Topic 8B	How EMPLOYEES' job duties and responsibilities changed or stayed the same while working from home;	The general job duties and responsibilities of call center employees while working from home during the relevant time period as a result of the pandemic.	
Topic 8C	The dates when EMPLOYEES were allowed to work at home and how that effects any testimony in Cat 1-7 above;	The approximate dates after which call center employees began working from home in 2020 in response to the pandemic.	

MUNGER, TOLLES & OLSON LLP

Richard E. Quintilone
 March 18, 2022
 Page 19

Topic 8D	Wells Fargo's policies and procedures re: working from home;	Any new or additional policies related to timekeeping and meal and rest breaks, if any, that were implemented for call center employees working from home as a result of the pandemic.	
Topic 8E	The configuration of EMPLOYEES' work stations while working from home (whether certain equipment is provided and what Wells Fargo provides and does not provide).		Limited by Court to how timekeeping was done while working from home. (26:3-6)

Best,



Martin D. Bern

MDB;jol